

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

UNITED STATES OF AMERICA

v.

VINCENT GALARZA

Defendant.

:
:
:
:
:
:
:

Magistrate No. 18-MJ-146

**GOVERNMENT’S MOTION TO RECONSIDER DEFENDANT’S BOND STATUS AND
TO SCHEDULE A HEARING ON OR BEFORE MAY 3, 2019**

The United States of America, by and through its attorney, the United States Attorney for the District of Columbia, respectfully submits this Memorandum in support of its request for the defendant, Vincent Galarza, to appear before this Court, have his pre-trial release revoked based on newly discovered evidence, and be detained pending trial in this matter. The defendant is charged by Complaint with one count of Conspiracy to Distribute Child Pornography, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1). At the time of the defendant’s arrest in the Eastern District of New York on December 11, 2018, the government requested pre-trial detention. The request was denied and the defendant is currently released on conditions pending trial in this matter.

However, following a recent forensic review of the defendant’s electronic devices that were seized at the time of his arrest, law enforcement has identified over 500 images and videos depicting child pornography, two of which are directly linked to the charged offense. Law enforcement has also identified eleven videos and approximately 900 images of a 14-year-old minor (CW1) that were surreptitiously recorded by the defendant between March and August 2014. These depictions capture the lascivious exhibition of the minor’s genitalia and pubic area as she unknowingly undressed and showered in the bathroom at her home. Following the

identification of the minor victim, law enforcement met with the victim's family members and were informed by W-1 that in January 2016, the defendant snuck into her sister's (CW2) bedroom while she was asleep, put a pellet gun to her head, and threatened to rape her.

While the full forensic review and investigation into the defendant's surreptitious production of child pornography remains on-going, the United States of America, by and through its attorney, the United States Attorney for the District of Columbia, submits this Memorandum in support of its request for the Court to reconsider and revoke the defendant's release status. The government requests that the Court schedule a hearing on this matter on or before May 3, 2019. The government submits that the defendant should be detained pending the trial of this matter pursuant to 18 U.S.C. §§ 3142(f)(1)(A) and (f)(1)(E), because there is no condition or combination of conditions that will reasonably assure the safety of any person and the community. An analysis of the factors set forth in 18 U.S.C. § 3142 leads to the conclusion that detention is appropriate.

PROCEDURAL BACKGROUND

On December 11, 2018, the defendant was arrested in the Eastern District of New York by way of a District of Columbia Complaint, charging him with one count of Conspiracy to Distribute Child Pornography, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1). The defendant was presented in the District Court for the Eastern District of New York later that day.

The government requested that the defendant be detained pursuant to 18 U.S.C. § 3142, but the Court granted the defendant's request to be released on bond and conditions. The government did not appeal the Court's decision. The defendant's release conditions include home confinement with GPS monitoring, limited Internet usage, restrictions on contact with minors, and a \$200,000 cash bond.

On December 19, 2018, the defendant appeared in the District Court for the District of Columbia for his initial appearance. Due to the evidence known to the government at that time, the government requested that his bond and release conditions remain the same.

FACTUAL BACKGROUND

A. Definition of Terms

The Tor Network

Tor is a computer network which anonymizes Internet activity by routing a user's communications through a global network of relay computers (or proxies), thus effectively masking the internet-protocol ("IP") address of the user. An "IP address" is a unique numeric address (used by computers on the internet) that is assigned to properly direct internet traffic. A publically visible IP address can allow for the identification of the user and his/her location.

To access the Tor network, a user has to install freely available Tor software, which relays only the IP address of the last relay computer (the "exit node"), as opposed to the user's actual IP address. There is no practical method to trace a user's actual IP address back through those Tor relay computers.

The Tor network makes it possible for a user to operate a special type of website, called "hidden services," which uses a web address that is comprised of a series of 16 algorithm-generated characters (such as "asdlk8fs9dfiku7f") followed by the suffix ".onion." Websites, including hidden services, have system administrator(s) (also called the "admin(s)") who are responsible for overseeing and operating these websites.

Bitcoin

Bitcoin ("BTC") is one type of virtual currency that is circulated over the Internet. BTC is not issued by any government, bank, or company but rather is controlled through computer

software. Generally, BTC is sent and received using a BTC “address,” which is like a bank account number and is represented by a case-sensitive string of numbers and letters. Each BTC address is controlled through the use of a unique private key, a cryptographic equivalent of a password. Users can operate multiple BTC addresses at any given time, with the possibility of using a unique BTC address for every transaction.

BTC fluctuates in value. Around March 5, 2018, one BTC was worth approximately \$11,573.00. A typical user purchases BTC from a BTC virtual-currency exchange, which is a business that allows customers to trade virtual currencies for conventional money (*e.g.*, U.S. dollars, euros, etc.). Little to no personally identifiable information about the sender or recipient is transmitted in a BTC transaction itself. However, virtual currency exchanges are required by U.S. law to collect identifying information of their customers and verify their clients’ identities.

To send BTC to another address, the sender transmits a transaction announcement, cryptographically signed with the sender’s private key, across the BTC network. Once the sender’s transaction announcement is verified, the transaction is added to the blockchain. The blockchain is a decentralized, public ledger that logs every BTC transaction. In some instances, blockchain analysis can reveal whether multiple BTC addresses are controlled by the same individual or entity. For example, analyzing the data underlying BTC transactions allowed for the creation of large databases that grouped BTC transactions into “clusters.” This analysis allowed for the identification of BTC addresses that were involved in transacting with the same addresses.

B. The Website

“The Website” was a website dedicated to the advertisement and distribution of child pornography that operated as a hidden service on the Tor network until March of 2018 when it

was seized by law enforcement. On or about September 28, 2017, February 8, 2018, and February 22, 2018, from a location in Washington, D.C. law enforcement agents accessed The Website and documented its content, which is described herein. The Website was used to host and distribute video files depicting child pornography that could be downloaded by site users. The Website was not intended to be used to upload pornography of adults, as evidenced on the upload page on The Website which clearly stated: “Do not upload adult porn.”

On the video search page of The Website, there was a list of keyword search terms and the number of videos associated with the keyword. When law enforcement accessed the contents of The Website on or about February 8, 2018, it was determined that some of the top keyword search terms included “PTHC” (over 10,000 videos), “PEDO” (over 7,000 videos), “2yo%” (over 4,000 videos) and “4yo%” (over 4,000 videos).

On or about February 8, 2018, The Website indicated on its download page details that its users had downloaded video files from The Website more than a million times. On or about March 5, 2018, The Website server had over 250,000 unique video files, which totaled approximately eight terabytes of data.

Any user could create a free account on The Website by creating a username and password. Only after the user registered an account could the user browse previews of videos available for download and post text to The Website. To download videos from the site, users used “points,” which were allocated to users by The Website. A registered user could earn points from The Website in several ways: (1) uploading videos depicting child pornography; (2) referring new users to The Website; (3) paying for a “VIP” account, which lasted for six months, entitled a user to unlimited downloads, and was priced at 0.03 BTC (approximately \$327.60 as of March 1, 2018);

or (4) paying for points incrementally (*i.e.*, .02 BTC for 230 points).¹ Points were not transferable to any other website or application.

Certain persons joined the conspiracy to distribute child pornography by uploading videos to The Website. Those co-conspirators who uploaded videos of child pornography to The Website for “points” also earned additional “points” each time a customer of the site downloaded that particular video from The Website. Thus, the co-conspirators had a shared goal as part of the conspiracy – increasing the number of unique videos on The Website to drive additional traffic to it, which in turn led to greater downloads and more points for the co-conspirators. When uploading videos, the co-conspirators would use explicit file names highlighting the content as showing the sexual exploitation of minors and would add tags that customers could search for, such as PTHC, 2yo, etc. In order to prevent duplicate videos from being uploaded, The Website operated a digital hash-value check of videos the co-conspirators uploaded in order to compare the video to other videos previously uploaded to the site. The Website did not allow a co-conspirator to upload a video whose hash value matched something previously uploaded to the site.

During the course of the investigation, law enforcement agents in Washington, D.C. accessed The Website on multiple occasions, including on or about September 28, 2017, February 8, 2018, and February 22, 2018, observed its functionality by browsing the listings on The Website, and conducted undercover purchases by downloading child pornography video files from The Website. These downloaded child pornography video files included pre-pubescent children, infants, and toddlers engaged in sexually explicit conduct. Each video available for download from The Website had a title, a description (if added by the co-conspirator), “tags” with further

¹ Bitcoin is volatile and the price of bitcoin can fluctuate on an hourly basis. Between January 2017 and February 2018, for example, 1 bitcoin fluctuated in price from approximately \$1,000 to \$20,000 USD.

descriptions of the video enabling a user to more easily locate a particular category of video using The Website's search function, and a preview thumbnail image that contained approximately sixteen unique still images from the video.

C. Investigation Of the Administrator Of The Website

On or about September 1, 2017, law enforcement reviewed the source code of The Website's homepage, which could be viewed by right-clicking on The Website in the Tor browser and selecting "View Page Source." In reviewing the source code, law enforcement discovered that The Website had failed to conceal an IP address, likely due to user error on the part of the administrator. This IP address resolved to a telecommunications provider in South Korea. Subsequent investigation confirmed that this IP address was registered in the name of Jong Woo Son and was serviced at his residence in South Korea.

On February 28, 2018, a federal magistrate judge in the United States District Court for the District of Columbia issued an arrest warrant for Jong Woo Son. On or about March 5, 2018, South Korean law enforcement executed a search warrant at the residence of Jong Woo Son in South Korea. Pursuant to the search, South Korean law enforcement seized The Website's server and associated electronic storage media from the bedroom of Jong Woo Son – The Website's administrator. South Korean law enforcement then provided to U.S. law enforcement a forensic image of the server. U.S. law enforcement subsequently obtained a federal search warrant to review this forensic image.

A review of the imaged data confirmed that The Website was hosted on the seized server. A review of a sample of the video files further corroborated that The Website was dedicated to the distribution of child pornography. The customer data generally identified which user was associated with which BTC payment to The Website. A review of the forensic image of the server

further revealed that certain customers that paid BTC into The Website were also co-conspirators who uploaded content to the site.

On August 8, 2018, a federal grand jury in the District of Columbia indicted Jong Woo Son on various counts, including Conspiracy to Distribute Child Pornography, in violation of 18 U.S.C. Sections 2252(a)(2) and (b)(1).

D. Identification of Co-Conspirator Galarza (A/K/A “thisthishold)”

A review of the forensic image of the server revealed a transfer of approximately 0.00228809 BTC (worth about \$1.80 at the time of transaction) on December 17, 2016 from a BTC address to The Website’s BTC address starting with 1Hrb. Subpoena returns from a virtual-currency exchange in the United States (“BTC Exchange”) revealed that the source of this BTC transfer was from BTC Exchange Account number starting with 5855 (“Subject BTC Exchange Account”).²

Law enforcement’s review of the forensic image of the server revealed that The Website created the BTC address starting with 1Hrb for a user account in the name of thisthishold. A review of co-conspirator thisthishold’s account revealed that between approximately May 31, 2017 and February 9, 2018, co-conspirator thisthishold downloaded approximately 174 videos from The Website with video file names and descriptions indicative of child pornography. Additionally, from approximately June 25, 2016 to December 21, 2016, co-conspirator thisthishold uploaded

² On December 17, 2016, the, Subject Exchange Account sent approximately 0.1025 BTC and 0.005 BTC (worth about \$80.97 and \$3.95 respectively at the time of transactions) to a BTC mixer. A BTC mixer is a paid service that attempts to obfuscate the trail of BTC by mixing multiple clients’ transactions together so that there is not a direct trail from the BTC sender to the recipient. On December 17, 2016, The Website BTC address starting in 1Hrb also received approximately 0.09882853 BTC from a mixer. It appears that the defendant attempted to fund his account at The Website for a 0.1 BTC VIP account by sending the approximate 0.1025 BTC. However, he did not account for the normal BTC transactional fees and the mixer’s fees. Thus, he had to send an additional smaller BTC amount from 1Hrb to The Website and he chose to forgo the mixer with his third transaction to The Website – *i.e.*, the approximately 0.00228809 BTC transaction described above.

approximately 560 videos to The Website – all of which are videos that depict child pornography.

For example, video file EA - N2016H-034.mp4 with file description “EA - N2016H-part” was uploaded to The Website by co-conspirator thisthishold on November 20, 2016. The video is 19 seconds long and depicts a female child, approximately five to seven years old, nude from the waist up. The child appears to be laying on her back while an adult male stands over her and masturbates his penis near her mouth until he ejaculates on her face. The video ends with a collage of photographs of the same child with semen on her face. Users of The Website downloaded this video approximately two times.

Another video, entitled 20150805201415-031.mp4 with the file description “20150805201415-part” was uploaded to The Website by co-conspirator thisthishold on December 20, 2016. The video is 24 seconds long and depicts a female child, approximately five to seven years old, nude from the waist down. The child appears to be laying on her back, viewing a computer tablet, while a male adult inserts the head of his penis into the child's vagina. Users of The Website downloaded this video approximately three times.

Subpoena returns from the BTC Exchange revealed that the Subject BTC Exchange Account (which sent BTC to The Website) was created on or about December 17, 2016 with the following know-your-customer data:

- registered in the name of VINCENT GALARZA (“defendant”);
- the defendant’s date of birth;
- the defendant’s address in Glendale, New York;
- the defendant’s phone number; and
- an email address of vinmanagent11@aim.com.

As part of the BTC Exchange’s legally required customer due diligence rules, the BTC Exchange confirmed this email address and phone number by sending messages to which the user

had to reply.

Subpoena returns from Oath revealed that the email address of vinmanagent11@aim.com was created on December 15, 2002 and is registered to Vincent Galarza (defendant) with the same telephone number that the defendant provided when he created the Subject BTC Exchange Account on December 17, 2016.

The Subject BTC Exchange Account was funded by a Cross County Savings Bank (“CCSB”) checking account ending in 0160 and a Chase Bank credit card ending in 8140. Subpoena returns revealed that both of these payment methods were listed in the defendant’s name. The subpoena returns further revealed that the defendant opened the account ending in 0160 in 2008. The defendant provided the same date of birth, phone number, and address when he opened his accounts that he had provided to the BTC Exchange when he opened the Subject BTC Exchange Account. The defendant had also provided copies of his driver’s license and Social Security card when he opened his account with CCSB as well. Subsequent law enforcement investigation identified CCSB ATM security footage from December 26, 2017, which depicts an individual resembling the defendant’s driver’s license photograph accessing a CCSB ATM.

NEWLY DISCOVERED EVIDENCE WARRANTING DETENTION

A. Defendant’s Additional Collection Of Child Pornography

At the time of the defendant’s arrest in New York, law enforcement executed a search warrant and seized several electronic devices, to include a self-built computer with a Redundant Array of Independent Disks (“RAID”) configuration. Note that “RAID” is a sophisticated way to pair multiple drives together to improve both performance and redundancy. A review of the self-built computer under the username “Vincent John Galarza” identified over 500 videos and images of child pornography, the majority of which depicted sexually explicit conduct of pre-

pubescent children. While the forensic review remains on-going, law enforcement has identified at least two videos that were uploaded by user “thisthishold” to The Website.

B. Defendant’s Production of Child Pornography

The forensic review of the defendant’s electronic devices also identified eleven videos of a 14-year old minor (CW1). CW1 has been identified as the defendant’s then-girlfriend’s younger sister. These videos were surreptitiously recorded between March and August 2014 and capture CW1 undressing and using the shower. In at least one of the videos, the defendant’s face is observed as he is setting up the camera. In another video, the defendant is observed examining the angle of the camera before exiting the bathroom. These eleven videos were then edited and clipped to produce over 900 still-shots that focus on the same minor’s genitalia and pubic area. (Note that law enforcement still has over 150,000 files to review before a final number can be obtained regarding videos and images of the minor.)

On April 19, 2019, law enforcement interviewed W-1, a family member of CW1. W-1 confirmed the identity and age of CW1. W-1 also identified that the location of these recordings was in CW1’s bathroom in her home in New York. W-1 further informed law enforcement that the defendant assisted the family with updates to all of the family’s electronic devices because he was computer-savvy. According to W-1, CW1 had a web-camera that had been set up on her computer. CW1 would often complain that the web-camera would switch on and off automatically when CW1 was in the room. CW1 believed that there was something wrong with the web-camera and ultimately the family got CW1 a new system. However, law enforcement identified on the defendant’s electronic device numerous still images that appear to have been from CW1’s web camera. These depictions show CW1 in various stages of undress with her breasts exposed.

Accordingly, it is believed that the defendant, while under the auspices of assisting CW1 with her computer and web-camera, used his expertise to hack into her system and commandeer her web-camera. This belief is supported by the fact that CW1's web camera was reported to go "on and off" without prompting, and the defendant has screen-shots of CW1 changing in her bedroom consistent with being recorded, surreptitiously, from CW1's web camera.

C. Defendant's Assaultive Conduct

During the interview of W-1, W-1 also disclosed an incident that had occurred at their home in New York on January 1, 2016. According to W-1, the defendant entered CW2's bedroom while CW2 (adult) was asleep. CW2 woke to find the defendant standing over her bed and he was holding a pellet gun to her head. CW2 informed W-1 that the defendant had threatened to rape her.³ CW2 yelled for help and W-1 came to her assistance. At that time, the defendant was removed from the house and according to W-1, he has not returned since.

APPLICABLE LEGAL STANDARD

The Bail Reform Act permits a judicial officer to hold an individual without bond pending trial if the officer finds clear and convincing evidence that "no condition or combination of conditions will reasonably assure the appearance of the person as required and the safety of any other person and the community." 18 U.S.C. § 3142(e). Pursuant to 18 U.S.C. § 3142(f)(1)(A), the judicial officer shall hold a hearing on the question of detention upon the motion of the government in a case that involves a crime of violence. The offense of Conspiracy to Distribute Child Pornography, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1), is a crime of violence because it is a felony under Chapter 110. See 18 U.S.C. § 3156(a)(4)(C). In addition, because

³ Note, however, that in the sealed police report, CW2 provided a statement to police at the time of the offense. She stated that she could not recall what the defendant had said to her.

the alleged offense in this case involve a minor victim, there is a rebuttable presumption in favor of detention. See 18 U.S.C. § 3142(e)(3)(E).

In making a detention determination, the Court must consider the following factors: (1) the nature and circumstances of the offense charged; (2) the weight of the evidence against the defendant; (3) the history and characteristics of the defendant; and (4) the nature and seriousness of the danger to any person or the community that would be posed by the defendant's release. See 18 U.S.C. § 3142(g).

Here, there is a rebuttable presumption that the defendant be held pending trial. Moreover, a consideration of the newly discovered evidence and all of the statutory factors weighs heavily in favor of detention.

ANALYSIS

For the reasons that follow, the government submits that no condition or combination of conditions will reasonably assure the safety of any other person and the community.

A. The Nature and Circumstances of the Offense Charged

The nature and circumstances of the charged offense has always favored detention. The defendant has been charged with an extremely serious offense that involves the trafficking of hundreds of videos of children being sexually abused. The harms to the children depicted in these videos cannot be overstated. As Congress found in enacting the Child Pornography Prevention Act of 1996, "the existence of and traffic in child pornographic images creates the potential for many types of harm in the community and presents a clear and present danger to all children." Pub. L. No. 104-208, § 121, 110 Stat. 3009 (codified at

Accordingly, due to the seriousness of this charge, a violation of Section 2252(a)(2) carries a minimum term of imprisonment of five years. See 18 U.S.C. § 2252(b)(1).

Here, the defendant sought out and actively participated in an online safe haven that fostered the mutual encouragement and promotion of the sexual exploitation of children. The defendant utilized a sophisticated method (Tor network) to evade detection of his activities. He not only downloaded these graphic and disturbing videos, but he contributed to the growing marketplace by uploading 560 videos to The Website.

Accordingly, the defendant, by his very conduct, has promoted and encouraged the sexual abuse of children and warrants detention.

B. The Weight of the Evidence Against the Defendant

Law enforcement has identified the defendant as being linked to the Subject BTC Account that paid into The Website and the “thisthishold” user who uploaded 560 videos of child pornography to The Website in exchange for “points” to download other videos of child pornography. However, following the forensic review of his electronic devices, the weight of the evidence against the defendant is overwhelmingly strong. As noted above, law enforcement has identified over 500 videos and images of child pornography on the defendant’s electronic device, where at least two videos were ones that user “thisthishold” had uploaded to The Website.

Accordingly, the weight of the evidence against the defendant is sufficient and equally warrants detention.

C. The History and Characteristics of the Defendant

While the defendant has no criminal history and initially, this factor weighed in favor of the defendant’s release, the newly discovered evidence depicts an individual who has been actively

engaged in the sexual exploitation of children and minors over the course of several years. The defendant's charged offense was not an aberration of character, but rather very much defines his character: that of a sexual predator.

Violating the trust of the family of his then-girlfriend, the defendant snuck into the minor's bathroom, secreted a recording device to capture her most intimate and personal moments, and then spent considerable time reviewing and editing these videos to screen-capture those images he was most interested in: images of her genitalia and pubic area. This, alone is concerning to the government, because it shows an individual who knows no boundaries and who is willing to target those people in his life who trust him the most. The defendant's production and trafficking of child pornography, coupled with CW2's allegation that the defendant, while armed with a pellet gun, threatened to rape her, demonstrates an individual who presents a danger to the community.

Accordingly, the defendant's history and characteristics, to wit: a producer of child pornography and a threatened rapist, weighs in favor of detention.

D. The Nature and Seriousness of the Danger to Any Person or the Community

The defendant's sophisticated use of Tor, mixers, and RAID configurations demonstrates that the defendant is a more sophisticated offender than the average CP-collector. The defendant has capitalized on a way to possess, distribute, and produce such material while minimizing the risk of getting caught. This makes the defendant the kind of person who is more difficult to monitor on pretrial release, as there are no forensic tools that could be run on his computers while on release to see if he has continued to access child pornography on the darknet – or whether he has commandeered another innocent minor's web-camera for his perverse viewing pleasure.

The defendant's surreptitious and voyeuristic recordings of CW1 is the clearest indicator

that he presents a significant danger to the community if he remains released. Due to the egregious nature of this additional allegation, a violation of 18 U.S.C. Section 2251 (Sexual Exploitation of a Minor) carries a minimum term of imprisonment of fifteen years. Certainly, had the government been aware of the defendant's production of child pornography, his threatening behavior towards CW2, and the large number of videos and images of child pornography in his possession at the time of his arrest, the government would have appealed the Eastern District of New York's release decision. Additionally, if the Court had been aware of the defendant's assaultive and exploitive conduct, the Court very well may not have agreed to release the defendant into the community.

IV. Conclusion

For all of the reasons set forth above, and any other reasons set forth at any hearing on this issue, a consideration of the evidence in this case and the applicable statutory factors compels the conclusion that the defendant's release conditions should be reconsidered and revoked and he should be detained pending trial.

Accordingly, the government requests that the Court schedule this matter for a hearing on or before May 3, 2019.

Respectfully submitted,

JESSIE K. LIU
UNITED STATES ATTORNEY

By: /s/
Lindsay Suttenger, D.C. Bar No. 978513
Assistant United States Attorney
555 Fourth Street, N.W.
Washington, D.C. 20001
(202) 252-7017
Lindsay.Suttenger@usdoj.gov